rieur de chacun, l'information quantique est convertie en information classique puis à nouveau sous forme quantique. Et pour éviter tout risque d'espionnage lorsque le signal est mis sous forme classique, chaque bâtiment est gardé par un bataillon de l'armée chinoise…

Moins gourmande en soldats et plus intéressante est l'idée d'utiliser un satellite, situé à quelque 500 kilomètres d'altitude, de sorte que la plus grande partie du parcours des photons émis vers la terre se fait dans le vide. Seuls les 10 kilomètres d'épaisseur de l'atmosphère donnent lieu à une absorption. C'est à ce jour l'unique méthode pour envoyer deux photons intriqués à 1200 kilomètres l'un de l'autre d'une traite. Je trouve ça très beau.

Faisons un peu de pédagogie. À quoi cela peut-il servir ?

Alain Aspect : À la cryptographie quantique ou à la téléportation quantique à grande distance, dans les deux cas en utilisant une paire de photons intriqués. Pour la cryptographie quantique, il s'agit de distribuer à deux partenaires, Alice et Bob, deux suites identiques de 0 et de 1, qui serviront de clés de cryptage et de décryptage. Les corrélations quantiques entre photons intriqués garantissent que les clés sont identiques, et qu'il est impossible, pour des raisons fondamentales, d'en obtenir une troisième copie.

Quant à la téléportation quantique, l'idée – très subtile – est la suivante. L'état d'un objet quantique est décrit, en mathématiques, par un vecteur dans ce que l'on appelle un espace de Hilbert. Cependant, la totalité de l'information sur cet état (disons les composantes de ce vecteur) est inaccessible à la mesure ; seule une partie de l'information (une projection du vecteur sur une base de dimension limitée) est à portée d'instrument. Dans ces conditions, il semble *a priori* impossible de connaître la totalité de l'état quantique d'un objet et d'envoyer l'information correspondante à distance. Eh bien la téléportation quantique, fondée sur l'intrication, permet de contourner ce problème !

Avec une paire de photons intriqués, on peut d'abord faire interagir le premier photon avec le système dont on veut téléporter l'état. Cet état se trouvera copié sur le second photon de la paire au terme d'une série d'opérations. De la sorte, l'état quantique aura voyagé. Cependant, il y a un prix à payer. L'état quantique du système de départ, téléporté, a été complètement modifié à l'issue des opérations : il a été « coupé-déplacé » sur le second photon et a été effacé du système de départ. Mais c'est quand même extraordinaire si l'on songe que l'état a été déplacé en totalité alors qu'on ne peut pas le connaître.

Cette téléportation rend possible un internet quantique, en tout cas un réseau d'ordinateurs quantiques qui échangeraient des états quantiques. Ce n'est pas la téléportation de matière, à la Star Trek, mais celle d'une information quantique. L'idée est fascinante.

Un problème encore mal résolu réside dans la nécessité d'une mémoire quantique, indispensable pour rendre vraiment efficace la téléportation quantique, car il faut garder en attente, jusqu'à la fin du processus, l'information partielle sur l'état quantique transférée « instantanément » lors de l'interaction avec le premier photon. Une mémoire quantique efficace aurait bien d'autres applications : elle permettrait de développer des répéteurs quantiques basés sur des photons intriqués, permettant de régénérer le signal quantique atténué dans les fibres optiques sans passer par un signal classique intermédiaire. Avec de tels répéteurs quantiques, on pourrait dépasser la limite des 100 kilomètres sans recourir à des satellites. Mais il n'existe pas encore de très bonne mémoire quantique, bien que sur le plan fondamental, rien ne semble s'y opposer.

L'autre grande information qui fait un peu de bruit est l'annonce de Google sur la suprématie quantique qu'ils auraient atteint. Comment y voir clair ?

Alain Aspect : Il faut d'abord dire que l'expérience réalisée est remarquable. On la doit à un scientifique exceptionnel, John Martinis, de l'université de Californie, à Santa Barbara, aux États-Unis, qui a longtemps travaillé avec Daniel Estève, un des leaders des supraconducteurs dans son laboratoire du CEA à Saclay, ainsi qu'avec Michel Devoret, maintenant à Yale. Mais il faut distinguer l'annonce tonitruante de Google de la conférence donnée par John Martinis à l'institut de technologie de Californie, dans un contexte universitaire : il est à juste titre très fier de son résultat, mais il ne le survend pas.

Peut-on rappeler ce qu'est la suprématie quantique ?

Alain Aspect : D'abord, le vocabulaire fait polémique. Le terme « suprématie » implique l'élimination de tous les concurrents. Je préfère parler d'« avantage », c'est-à-dire une supériorité seulement dans certains types d'applications. Quoi qu'il en soit, avantage ou suprématie, c'est l'idée théorique selon laquelle on pourrait mettre en œuvre le parallélisme massif offert par l'intrication quantique pour réaliser des calculs beaucoup plus vite qu'avec une machine classique. Par « beaucoup plus vite », il faut entendre exponentiellement plus vite, au vrai sens scientifique du terme.

Prenons l'exemple de la factorisation des nombres entiers. Pour un nombre de 100 chiffres, un ordinateur classique aura besoin d'un temps T, et ce temps doublera pour un nombre de 101 chiffres, et doublera encore pour 102, etc. Le temps croît de façon exponentielle, et c'est cette croissance exponentielle qui permet de se mettre à l'abri des espions au fur et à mesure des progrès des ordinateurs.

Or on peut démontrer qu'en mettant en œuvre un algorithme particulier (celui de Shor) sur un ordinateur quantique, le temps de calcul d'une factorisation croît notablement plus lentement avec le nombre de chiffres. Ainsi, en renversant le point de vue, l'ordinateur quantique va exponentiellement plus vite que l'ordinateur classique.

Démontrer l'avantage quantique consiste à pouvoir dire : « J'ai résolu, avec un système quantique, un problème dont >

Pour éviter tout risque d'espionnage, chaque bâtiment est gardé par un bataillon de l'armée chinoise